CLAIMS

What is claimed is:

1. A method comprising:

receiving a CRUable U-NII radio card into an interface slot within a wireless ready device designed for receiving radio cards, said radio card having a radio identification (ID) parameter, wherein said slot enables said radio to be electrically coupled to and interface with an antenna that is embedded in the device and has an antenna identification (ID) parameter;

during boot up of the device, completing an authentication process utilizing a table within a BIOS of the device of paired radio-antenna IDs for authorized radio-antenna combinations, wherein the authentication process verifies that said radio is an authorized radio for utilization with the antenna within the device under U-NII standards; and

when said authentication process verifies that said radio is authorized, completing a boot of said device and enable U-NII communication via the combination of said antenna and said radio, wherein a U-NII transmitter meeting an FCC "integral" requirement is provided within the wireless ready device having an embedded antenna.

2. The method of Claim 1, wherein:

said CRUable U-NII radio is fabricated on a wireless module that also comprises a register holding the radio ID and an interface for connecting to said interface slot of said device;

said device comprises the antenna, the interface slot, a coax connector slot and coax coupling the connector slot to said antenna, a basic input/output system (BIOS) with a table of approved radio-antenna pairings and an OEM field with a secret key programmed by a manufacturer; and

said step for completing an authentication process completes a radio-to-antenna and a radio-to-device authentication process, wherein only a correct radio model is enabled.

3. The method of Claim 1, said authentication process further comprising:

following a power on of said device, initiating a BIOS check of system components, wherein the radio ID is read from the CRUable U-NII radio that is also electrically coupled to said BIOS;

populating the table within system BIOS with authorized antenna-radio ID pairs for that device;

retrieving the antenna ID from a storage location within said BIOS;

reading a first radio ID from the table within the BIOS, wherein said radio PCI ID read is one stored as a paired entry in said table with the retrieved antenna ID of the embedded antenna;

comparing a pairing of said radio ID and said antenna ID against the table of approved radio/antenna ID pairs, wherein the radio IDs are compared once the retrieved antenna ID is located within the table.

4. The method of Claim 1, said authentication process further comprising:

retrieving a secret key from an OEM field within said BIOS, said secret key being an allowable card ID for that device, which is encrypted and stored in said OEM field by a manufacturer of said device;

decrypting said secret key;

comparing said secret key against card IDs within the table matching the ID of the CRUable U-NII radio card; and

enabling said radio to operate within said device only when said secret key matches the card ID, wherein U-NII transmission via the radio-antenna combination is enabled only when said radio-antenna ID pairing matches one of said approved radio/antenna ID pairs within the table and said secret key matches the ID of the connected radio card.

5. The method of Claim 4, said comparing step comprises comparing said secret key to a radio ID within said table within the BIOS.

6. The method of Claim 2, wherein said radio ID and said antenna ID are peripheral component interconnect (PCI) identifications (IDs).

7. The method of Claim 3, further comprising:

when said first radio ID and said second radio ID matches, allowing a boot process being executed on the device to complete, wherein when said match does not occur, said boot process is terminated.

8. The method of Claim 3, further comprising:

when said first radio ID and said second radio ID does not match, disabling said radio from operating within said device, wherein said device is booted without U-NII transmission capability.

9. The method of Claim 4, wherein said secret key authentication is completed proximate in time to said comparison of radio PCI ID pairs, whereby a dual authentication process is completed to activate said radio for U-NII operation within the device.

10. The method of Claim 3, wherein said enabling step further comprises:

storing an indication of said match within an approval flag;

checking said approval flag for said indication prior to completing a U-NII connection from said device, wherein a request for U-NII connection is allowed to proceed only when said approval flag indicates that U-NII connection is authorized and said secret key matches the card ID; and

clearing said approval flag whenever a triggering condition is registered on the device, said triggering condition being a condition form among rebooting the device, removing the wireless module, breaking a connection between said antenna and said radio, modification/replacement of said radio, modification/replacement of said antenna.

11. A wireless-ready device comprising:

an embedded antenna having an antenna ID and specific design characteristics to enable U-NII transmission when coupled to an authorized U-NII radio;

an interface which receives a CRUable U-NII radio card with a radio having a radio ID, wherein said interface enables said radio to be electrically coupled to and interface with the embedded antenna;

a BIOS that comprises an OEM field and a table of radio ID and antenna ID pairs for authorized U-NII radio-antenna combinations, said OEM field storing an encrypted allowable card ID;

an authentication mechanism associated with said BIOS that initiates a radio-to-device verification process during boot up of the device that verifies that said radio is an authorized

radio for utilization with the embedded antenna and within said device according to pre-established U-NII standards; and

U-NII transmitter activation logic that, when said verification process verifies that said radio is authorized for utilization with said antenna and within said device, for completing a boot of said device and enabling U-NII communication via the combination of said antenna and said radio, wherein a U-NII transmitter meeting an FCC "integral" requirement is provided within the wireless ready device.

12. The device of Claim 11, wherein:

said CRUable U-NII radio is fabricated on a wireless module that also comprises a register holding the radio ID and an interface for connecting to said interface slot of said device;

said device comprises the antenna, the interface slot, a coax connector slot and coax coupling the connector slot to said antenna, a basic input/output system (BIOS) with a table of approved radio-antenna pairings and an OEM field with a secret key programmed by a manufacturer; and

said authentication mechanism provides both radio-to-antenna authentication and radio-to-device authentication, such that only an authorized radio within an approved device is enabled.

13. The device of Claim 12, wherein said BIOS further comprising:

activation code, which initiates a BIOS check of system components following a power on of said device, wherein the radio ID is read from the CRUable U-NII radio that is also electrically coupled to said BIOS;

authentication code that (1) populates the table within system BIOS with authorized antenna-radio ID pairs for that device; (2) retrieves the antenna ID from a storage location within said BIOS; and (3) reads a first radio ID from the table within the BIOS, wherein said radio ID read is one stored as a paired entry in said table with the retrieved antenna ID of the embedded antenna;

a comparator that compares a pairing of said radio ID and said antenna ID against the table of approved radio/antenna ID pairs, wherein the radio IDs are compared once the retrieved antenna ID is located within the table; and

a verification mechanism that, when said first PCI ID and said second PCI ID matches, signals an approval of said radio-to-device authentication as a successful authentication of said radio for operation within said device.

14. The device of Claim 12, further comprising:

a device driver that controls access to and from said radio card, and which completes a radio-to-device authentication by:

retrieving a secret key from an OEM field within said BIOS, said secret key being an allowable card ID for that device, which is encrypted and stored in said OEM field by a manufacturer of said device;

decrypting said secret key;

comparing said secret key against card IDs within the table matching the ID of the CRUable U-NII radio card; and

enabling said radio to operate within said device only when said secret key matches the card ID, wherein U-NII transmission via the radio-antenna combination is enabled only when said radio-antenna ID pairing matches one of said approved radio/antenna ID pairs within the table and said secret key matches the ID of the connected radio card.

15. The device of Claim 13, further comprising:

boot termination mechanism that allows a boot process being executed on the device to complete when said first radio ID and said second radio ID matches, wherein when said match does not occur, said boot termination mechanism terminates said boot process.

16. The device of Claim 13, further comprising:

a transmission disabling mechanism that disables said radio from operating within said device when said first radio ID and said second radio ID does not match or said secret key does not match the card ID, wherein said device is booted without U-NII transmission capability.

17. The device of Claim 14, wherein said device driver comprises a transmission disabling mechanism that disables said radio from operating within said device when said first PCI ID and said second PCI ID do not match or said secret key does not match said card ID, wherein said

device is booted without U-NII transmission capability.

18. The device of Claim 16, further comprising:

a validation register that stores a result of the comparison of the radio IDs;

means for checking said validation register for said result prior to completing a U-NII connection with said device, wherein a request for U-NII connection is allowed to proceed only when said result indicates a match between said radio IDs; and

reset mechanism for resetting a value of said validation register whenever a triggering condition is registered on the device, said triggering condition being a condition from among rebooting the device, removing the wireless module, breaking a connection between said antenna and said radio, modification/replacement of said radio, modification/replacement of said antenna.

19. In a device having an embedded antenna designed for supporting wireless communication via the U-NII wireless protocol, a basic input/output system (BIOS), and an interface for electrically coupling a CRUable U-NII radio, a method for providing an authorized U-NII transmitter within the device, said method comprising:

detecting at the interface an electrical coupling to a CRUable mPCI card containing a U-NII-standard radio having an associated radio PCI ID and other identifying characteristic;

comparing the radio's PCI ID with a second radio PCI ID obtained from a table of radio-antenna PCI ID pairs corresponding to authorized U-NII radio-antenna combinations, wherein said table is provided within the BIOS of the device and said second radio PCI ID is selected by matching the antenna ID of the embedded antenna with a similar antenna ID within the table;

enabling U-NII transmission via the combination of the radio and the antenna only when said radio IDs match, indicating an approved combination of said radio and said embedded antenna.

20. The method of Claim 19, said comparing step further comprising:

following a power on of said device, initiating a BIOS check of system components, wherein the radio ID is read from the CRUable U-NII radio that is also electrically coupled to said BIOS;

populating the table within system BIOS with authorized antenna-radio ID pairs for that

device;

retrieving the antenna ID from a storage location within said BIOS;

reading a first radio ID from the table within the BIOS, wherein said radio PCI ID read is one stored as a paired entry in said table with the retrieved antenna ID of the embedded antenna;

comparing a pairing of said radio ID and said antenna ID against the table of approved radio/antenna ID pairs, wherein the radio IDs are compared once the retrieved antenna ID is located within the table.

21. The method of Claim 20, further comprising terminating said boot up when said comparison indicates the radio's ID does not match one within the table of approved radio-antenna ID pairs selected by matching the antenna ID.

22. The method of Claim 19, said authentication process further comprising:

retrieving a secret key from an OEM field within said BIOS, said secret key being an allowable card ID for that device, which is encrypted and stored in said OEM field by a manufacturer of said device;

decrypting said secret key;

comparing said secret key against card IDs within the table matching the ID of the CRUable U-NII radio card; and

enabling said radio to operate within said device only when said secret key matches the card ID, wherein U-NII transmission via the radio-antenna combination is enabled only when said radio-antenna ID pairing matches one of said approved radio/antenna ID pairs within the table and said secret key matches the ID of the connected radio card.

23. The method of Claim 22, wherein said secret key is a model number of approved cards for operation within the device and said model number is associated with the radio PCI ID within the table.

24. The method of Claim 22, wherein said enabling step further comprises:

storing an indication of said match of radio IDs within said an approval flag;

checking said an approval flag prior to completing an U-NII connection with said device,

wherein a request for U-NII connection is allowed to proceed only when said approval flag indicates the radio has been authenticated; and

clearing said approval flag whenever a triggering condition is registered on the device, said triggering condition being a condition form among rebooting the device, removing the wireless module, breaking a connection between said antenna and said radio, modification/ replacement of said radio, modification/replacement of said antenna.

25. The method of Claim 21, wherein said device is a portable computer system.